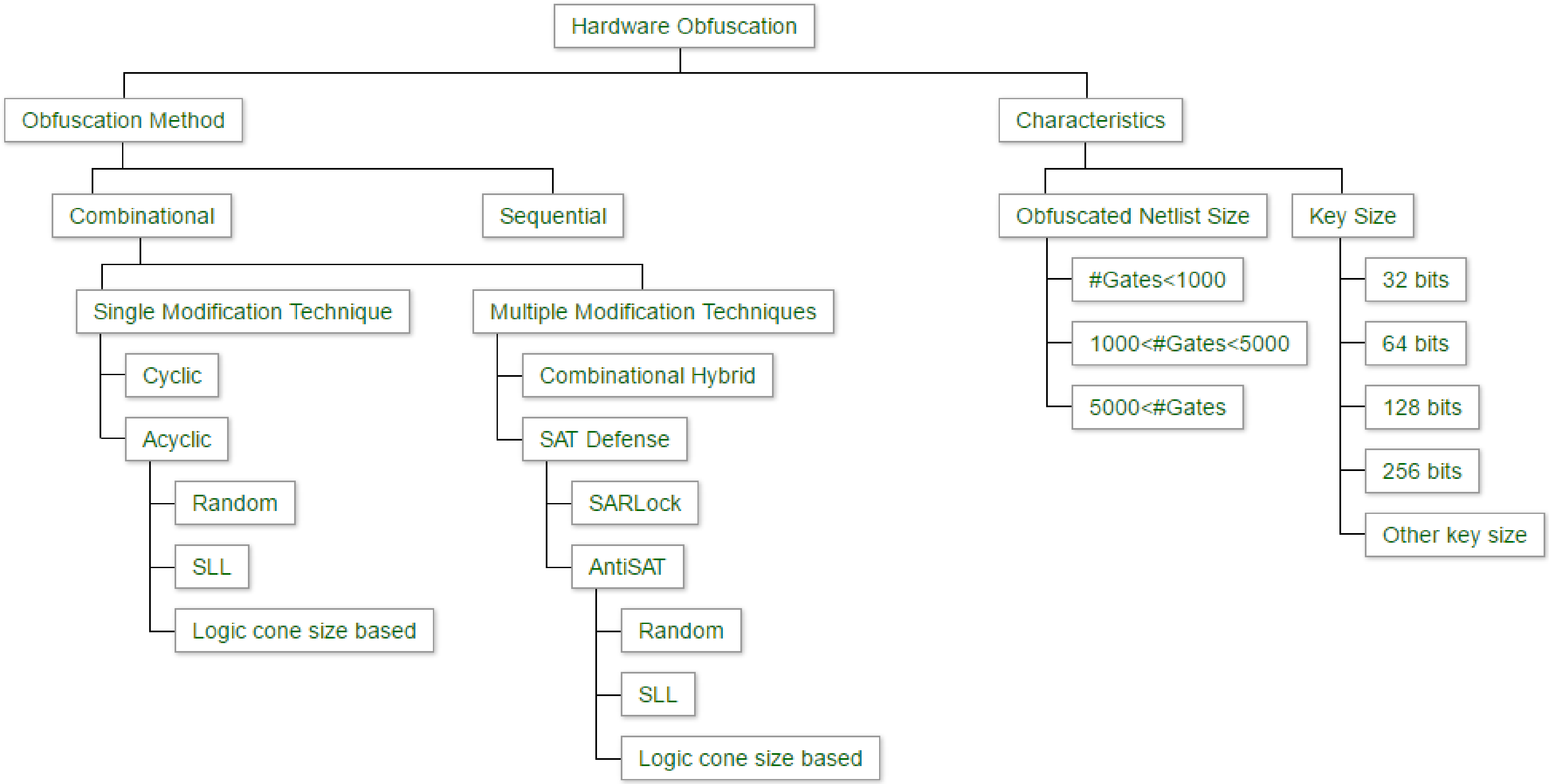
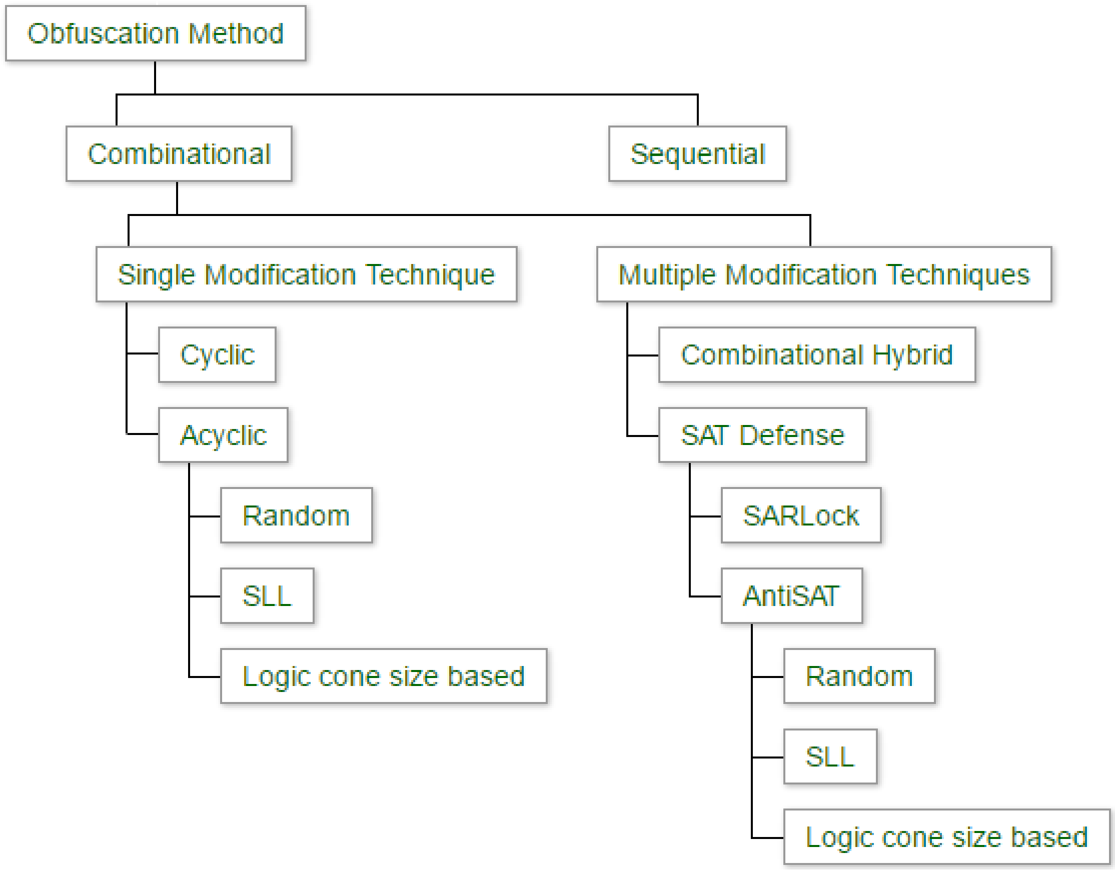
Hardware Obfuscation Taxonomy



- Hardware Obfuscation
  - Obfuscation Method
    - Combinational
      - Single Modification Technique
        - Cyclic
        - Acyclic
          - Random
          - SLL
          - Logic cone size based
      - Multiple Modification Techniques
        - Combinational Hybrid
        - SAT Defense
          - SARLock
          - AntiSAT
            - Random
            - SLL
            - Logic cone size based
    - Sequential
  - Characteristics
    - Obfuscated Netlist Size
      - #Gates<1000
      - 1000<#Gates<5000
      - 5000<#Gates
    - Key Size
      - 32 bits
      - 64 bits
      - 128 bits
      - 256 bits
      - Other key size

Based on obfuscation method:



- Obfuscation Method
  - Combinational
    - Single Modification Technique
      - Cyclic
      - Acyclic
        - Random
        - SLL
        - Logic cone size based
    - Multiple Modification Techniques
      - Combinational Hybrid
      - SAT Defense
        - SARLock
        - AntiSAT
          - Random
          - SLL
          - Logic cone size based
  - Sequential

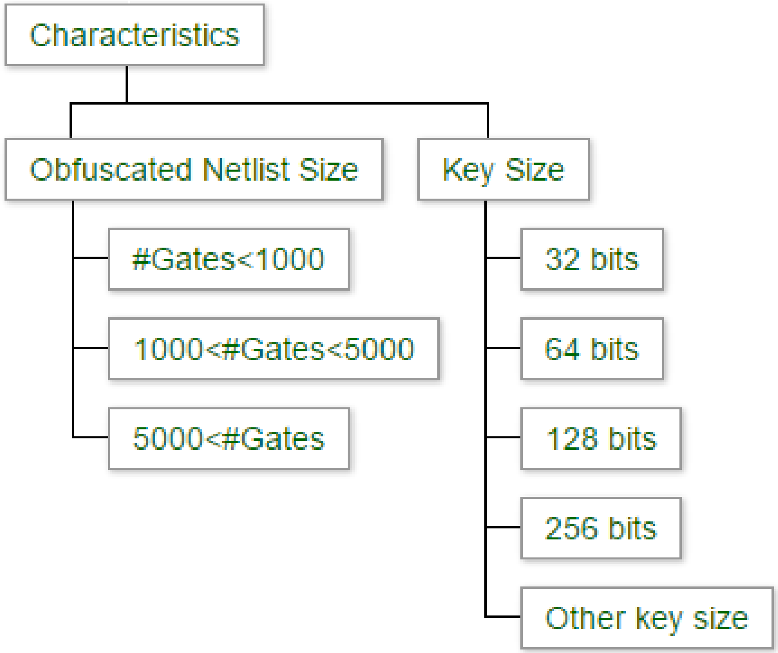
Hardware obfuscation can be divided into two groups – Combinational and Sequential Obfuscation.

The one or more combinational obfuscation methods can be applied simultaneously on a circuit.

Single techniques can be either cyclic[6] or acyclic. The acyclic techniques applied for generating obfuscation were Random insertion, Secure Logic Locking[1], and Logic Cone Size based[2].

Multiple modifications can be coupling with SAT attack[3] resiliency block or using multiple obfuscation methods. The SAT resiliency block can be AntiSAT[4], SARLock[5], or any other technique. These blocks can be applied along with other combinational obfuscation blocks.

Based of physical characteristics of the obfuscated benchmark



- Characteristics
  - Obfuscated Netlist Size
    - #Gates<1000
    - 1000<#Gates<5000
    - 5000<#Gates
  - Key Size
    - 32 bits
    - 64 bits
    - 128 bits
    - 256 bits
    - Other key size

Based on the size, the obfuscated circuits are categorized into three groups – with less than thousand gates, with more than a thousand but less than five thousand gates, and with more than five thousand gates. The size for benchmarks of acyclic and multiple methods are the size of corresponding synthesized benchmarks.

The combinational obfuscation has been done with 32 bit, 64 bit, 128 bit, and 256 bit keys.

Any benchmark that does not have key size as mentioned above is enlisted in the other key size group. In case of SAT resiliency technique, the AntiSAT methods are implemented with key size equal to the number of inputs and then 25% additional keys are added to obfuscate the AntiSAT block. The cyclic obfuscation benchmarks are also in this category.

References:

[1] Yasin, Muhammad, et al. "On improving the security of logic locking." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 35.9 (2016): 1411-1424

[2] Narasimhan, Seetharam, Rajat Subhra Chakraborty, and Swarup Chakraborty. "Hardware IP protection during evaluation using embedded sequential trojan." IEEE Design & Test of Computers 29.3 (2012): 70-79

[3] Y. Xie and A. Srivastava. Mitigating SAT attack on logic locking. In Proceedings of 18th Intl.Conf. on CHES 2016, Santa Barbara, CA, USA, 2016, pages 127-146, 2016

[4] Xie, Yang, and Ankur Srivastava. "Mitigating sat attack on logic locking." International Conference on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 2016

[5] M. Yasin, B. Mazumdar, J. J. V. Rajendran, and O. Sinanoglu. Sarlock: SAT attack resistant logic locking. In IEEE Intl. Symposium on HOST 2016, McLean, VA, USA, 2016, pages 236-241, 2016

[6] Shamsi Kaveh, Meng Li, Travis Meade, Zheng Zhao, David Z. Pan, and Yier Jin. "Cyclic obfuscation for creating sat-unresolvable circuits." In Proceedings of the on Great Lakes Symposium on VLSI 2017, pp. 173-178. ACM, 2017

Contact:

Sarah Amir

Florida Institute for Cybersecurity (FICS) Research

University of Florida

sarah.amir@ufl.edu, prema_buet@gmail.com